cafii acifa
The Canadian Association of Financial Institutions in Insurance | L'association canadienne des institutions financières en assurance

200-411 Richmond Street E, Toronto, ON M5A 3S5
☎ (416) 494-9224 🖷 (416) 967-6320
info@cafii.com www.cafii.com

March 1, 2022

Ms. Saskia Tolsma
Vice President, Stakeholder Engagement
BC Financial Services Authority
600-750 West Pender Street
Vancouver, B.C. V6C 2T8
policy@bcfsa.ca

Dear Ms. Tolsma:

Re: CAFII Feedback on BCFSA *Discussion Paper: Information Security Incident Reporting*

CAFII thanks BCFSA for the opportunity to provide feedback comments on the Authority's *Discussion Paper: Information Security Incident Reporting.*

We also thank you, Rob O'Brien, and Steven Wright for the information exchange meeting on the Discussion Paper which our Association had with you as BCFSA staff executives on February 24. The more than 15 CAFII representatives who participated found the meeting to be very informative and valuable. The insights and perspectives we exchanged prompted our Association to amend our written feedback comments in this final version of our submission. We also thank you and your colleagues for granting CAFII's request for a brief submission deadline extension of two business days to March 1, 2022.

CAFII understands and supports the important regulatory outcomes which BCFSA is seeking to achieve through its Information Security Incident Reporting initiative.

Our feedback below is divided into two sections: beginning with general *High Level Feedback and Resulting Recommendations*; followed by *Specific Feedback On Matters Raised In The Discussion Paper*.

High Level Feedback and Resulting Recommendations

CAFII has a critically important point of feedback to convey to BCFSA related to its desired outcome of being notified of information security incidents, one which arises from the intersection and overlapping which exists between provincial/territorial regulation of insurance and federal regulation of products and services offered by federally regulated financial institutions (FRFIs).

CAFII members, which are mainly the insurance arms of Schedule I Canadian banks and their insurer/underwriter partners, operate across the country in the life and health insurance sector; and, as such, they are provincially/territorially regulated. However, as federally regulated financial institutions (FRFIs), banks, some credit unions, and many insurers are also subject to federal regulation, including by the Office of the Superintendent of Financial Institutions (OSFI).

200-411 Richmond Street E, Toronto, ON M5A 3S5
☎ (416) 494-9224 🖷 (416) 967-6320
info@cafii.com www.cafii.com

Due to the fact that our Association's members are subject to both federal and provincial/territorial regulation (some 17 regulatory authorities in total, across the country), CAFII constantly requests of regulators that they harmonize their expectations of regulated entities to the maximum extent possible.

Often, regulators in different provinces introduce regulatory requirements which have the exact same intent as existing requirements in another province or federally, but yet which differ slightly in the details of how those expectations are defined, or are to be implemented and/or reported on by regulated entities.

In such cases, regulated entities have to allocate significant resources to deciphering and adjusting to the nuanced differences from jurisdiction to jurisdiction. This time-consuming, costly, and attention-sapping "exception management" process diverts resources away from the essential consumer protection aspects of regulators' expectations; and, in the case of an information security incident, away from investigating and resolving the incident for the benefit of affected consumers.

CAFII views BCFSA's *Discussion Paper: Information Security Incident Reporting* to be an example of the above-noted problem that significantly affects our members and other regulated entities.

There already exists a well-established, widely accepted and complied with, and effective OSFI Technology and Cyber Security Incident Reporting Advisory. OSFI's current Advisory came into force on August 16, 2021, replacing a predecessor version which was published on March 31, 2019. The OSFI Advisory includes all of the Information Security Incident Reporting dimensions which BCFSA covers in its Discussion Paper, including the following: definition of an information security incident; initial reporting requirements (which, identical to BCFSA's proposal, requires reporting within 24 hours of the regulated entity's determination that an information security incident has occurred); subsequent reporting requirements; the consequences of failure to report; examples of reportable incidents; and a form to use for reporting incidents.

Based on the foregoing relevant background context (and, as well, on the issues, concerns, and opportunities discussed in our February 24 meeting with BCFSA), CAFII makes the following inter-related recommendations to the Authority:

- Recommendation #1: BCFSA should lead an initiative at the Canadian Council of Insurance Regulators (CCIR), the national co-ordinating body of provincial/territorial insurance regulators, to develop one national Guideline/Guidance dealing with Information Security Incident Reporting, which would contain clearly specified triggers and requirements for the reporting of material, significant information security incidents.

  That Guideline/Guidance would be developed on a harmonized, national basis akin to the "Guidance: Conduct of Insurance Business and Fair Treatment of Customers" which was jointly developed by CCIR and CISRO and released publicly in September 2018, with shared, multi-jurisdiction compliance monitoring mechanisms built-in which give the Guidance the force and effect of a national Rule.

200-411 Richmond Street E, Toronto, ON M5A 3S5
☎ (416) 494-9224 🖷 (416) 967-6320
info@cafii.com www.cafii.com

The reporting template/vehicle developed to support the Guideline/Guidance would be akin to CCIR's very successful and nationally harmonized Annual Statement on Market Conduct (ASMC), except that reporting would be triggered immediately by a material information security incident, rather than being an annual, aggregation-type of reporting. This nationally standardized reporting mechanism would provide significant harmonization and efficiency benefits for regulated entities, and at the same time create a central and comprehensive repository of national information security incident data for regulators, data which could readily be used to conduct aggregated trends analyses and facilitate any regulatory follow-up that may be required.

The reporting requirements set out in this new Guideline/Guidance would prevail under and be beneficial for all provincial/territorial regulators, regardless of whether a particular jurisdiction has Rule-Making Authority or not.

- Recommendation #2: That the Guideline/Guidance to be developed by CCIR, under BCFSA's leadership/initiative, should utilize OSFI's current Technology and Cyber Security Incident Reporting Advisory and its related reporting form, to the maximum extent possible, as its model and template.

  Any additional information security incident data which provincial/territorial regulators may require to be reported, such as the number of provincial/territorial consumers affected by the incident, in order to meet their market conduct oversight responsibilities – given that OSFI's reporting template is concerned only with prudential regulatory issues – can be addressed simply by adding additional fields to the OSFI reporting template.

In keeping with the above-noted Recommendations, CAFII's view is that BCFSA ought not to use its Rule-Making Authority to introduce a BC-unique/specific Information Security Incident Reporting Rule when a nationally harmonized Guideline/Guidance approach – akin to the already proven CCIR/CISRO FTC Guidance and CCIR ASMC mechanisms – would be much more optimal for all stakeholders including -- indirectly but undoubtedly -- consumers.

In that connection (and to elaborate on a point briefly discussed in our February 24 meeting), CAFII and its members strongly disagree with the proposition that Guidelines are viewed as optional by the industry. We believe that Guidelines – whether regulator-issued Guidelines or industry Guidelines and voluntary commitments such as CLHIA Guidelines and the Canadian Bankers Association (CBA) Code of Conduct For Authorized Insurance Activities – constitute requirements. Compliance with Guidelines is a must and CAFII members strive to comply fully.

200-411 Richmond Street E, Toronto, ON M5A 3S5
☎ (416) 494-9224 🖷 (416) 967-6320
info@cafii.com www.cafii.com

Turning now to contingency options, should BCFSA find that taking on the leadership mantle at CCIR in developing a nationally harmonized Guideline/Guidance is not something that it can contemplate at this time, CAFII would recommend that (i) BCFSA strongly encourage another well-resourced regulator at the CCIR table – such as Ontario's FSRA or Quebec's AMF – to lead that national harmonization initiative; and (ii) should advocacy for a nationally harmonized initiative not find fertile ground at CCIR, then BCFSA should still seek to adopt the essence of CAFII's Recommendation #2 and our related commentary: i.e. the Authority should utilize OSFI's Technology and Cyber Security Incident Reporting Advisory and its related reporting form as its model and template, replicating it in an updated BC Guideline/Guidance on Information Security Incident Reporting to the maximum extent possible. Any additional data which BCFSA may require to be reported in order to meet the Authority's market conduct oversight responsibilities, such as the number of BC consumers affected by an incident, can be addressed simply by adding additional fields to the OSFI reporting template.

In summary, both the optimal nationally harmonized approach which CAFII advocates and the somewhat less optimal *harmonized-with-OSFI-only* approach would allow BCFSA to achieve its regulatory objectives with respect to information security incident reporting without imposing a largely new set of requirements upon regulated entities doing business in BC; and would thereby spare them from the costly inefficiencies which duplicative, yet slightly different regulations create.

Specific Feedback On Matters Raised In The Discussion Paper

CAFII is comfortable with BCFSA sharing information on patterns or trends which it may detect through an analysis of IS incident reports, via an aggregated, anonymized report. However, in that connection, our strongly held view is that the optimal approach for such information-sharing would be through an ASMC-like nationally standardized reporting mechanism as described in our Recommendation #1 above. We also believe that CCIR's sharing (optimal) or BCFSA's sharing (less optimal) of such reports periodically with the industry should be an important component of market conduct activities in this area.

While we are comfortable with BCFSA differentiating between two classes of institutions with respect to information security incidents, we question why the reporting requirements would be different for the two classes of institutions. We acknowledge that BCFSA's supervisory authority may differ between the two classes of institutions, but we fail to see why that fact should give rise to differentiated incident reporting requirements.

With respect to the sanctions and penalties that BCFSA proposes to have at its disposal with respect to information security incident reporting, CAFII strongly recommends that the Authority take a more measured approach than is outlined in the Discussion Paper. Particularly with respect to first/initial instances of non-compliance, we recommend that non-compliant financial institutions not be subject to possible administrative penalties of up to $50,000. We believe that a more collaborative and phased approach would be appropriate; and, in that connection, we note OSFI's approach to non-compliance:

> *Failure to report incidents as outlined above may result in increased supervisory oversight including but not limited to enhanced monitoring activities, watch-listing or staging of the FRFI. (Page 3.)*

200-411 Richmond Street E, Toronto, ON M5A 3S5
☎ (416) 494-9224 🖷 (416) 967-6320
info@cafii.com www.cafii.com

Conclusion

CAFII again thanks BCFSA for the opportunity to provide input and feedback on the Authority's *Discussion Paper: Information Security Incident Reporting.* Should you require further information from CAFII or wish to meet with representatives from our Association on this or any other matter at any time, please contact Keith Martin, CAFII Co-Executive Director, at keith.martin@cafii.com, or 647.460.7725.

Sincerely,

Rob Dobbins
Board Secretary and Chair, Executive Operations Committee

About CAFII

The Canadian Association of Financial Institutions in Insurance (CAFII) is a not-for-profit industry Association dedicated to the development of an open and flexible insurance marketplace. Our Association was established in 1997 to create a voice for financial institutions involved in selling insurance through a variety of distribution channels. Our members provide insurance through client contact centres, agents and brokers, travel agents, direct mail, branches of financial institutions, and the internet.

CAFII believes consumers are best served when they have meaningful choice in the purchase of insurance products and services. Our members offer credit protection, travel, life, health, and property and casualty insurance across Canada. In particular, credit protection insurance and travel insurance are the product lines of primary focus for CAFII as our members' common ground.

CAFII's diverse membership enables our Association to take a broad view of the regulatory regime governing the insurance marketplace. We work with government and regulators (primarily provincial/territorial) to develop a legislative and regulatory framework for the insurance sector which helps ensure that Canadian consumers have access to insurance products that suit their needs. Our aim is to ensure that appropriate standards are in place for the distribution and marketing of all insurance products and services.

CAFII's members include the insurance arms of Canada's major financial institutions – BMO Insurance; CIBC Insurance; Desjardins Insurance; National Bank Insurance; RBC Insurance; ScotiaLife Financial; and TD Insurance – along with major industry players Assurant; Canada Life Assurance; Canadian Premier Life Insurance Company; Canadian Tire Bank; CUMIS Services Incorporated; Manulife (The Manufacturers Life Insurance Company); Sun Life; and Valeyo.